



G. H. Raison College of Engineering & Management, Pune.

Department of Computer Engineering



Vulnerable University

Guide : - Prof. Gayatri Bedre

Presented By : -

► BCOA03 – Abhishek Birdawade

► BCOB93 – Srushti Deshpande

► BCOB111 – Vaibhav Wagh

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Contents

1. Introduction
2. Literature Survey
3. Existing System
4. Problem Statement
 - Proposed System
 - Objectives
 - System Architecture Diagram
 - Modules
 - Algorithm/Technology Used
 - UML Diagram
 - Hardware & Software Used
5. Advantages & Disadvantages
6. Applications
7. Conclusion
8. References



Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

RAISONI
GROUP OF INSTITUTIONS

Introduction



- Cyber criminals are more sophisticated, changing the attacking approach and they are creating a really crucial conditions for organizations by affecting their image.
- The vulnerable web applications can be used by web developers, security auditors, and penetration testers to practice their knowledge and skills during training sessions (and especially afterwards), as well as to test at any time the multiple hacking tools and offensive techniques available, in preparation for their next real-world engagement.
- Vulnerable applications available to security professionals for hacking, offensive and defensive activities, so that they can manipulate realistic web environments... **without going to jail** 😊.
- Security Professionals can practice and enhance their skills regarding web application security testing by learning and practicing about various technical and non-technical bugs and vulnerabilities.

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

Literature Survey

| Sr. No. | Paper Title | Author Name | Date | Findings |
|---------|---|---|------------|--|
| 1. | Security Testing: A Survey | Michael Felderer, Matthias Büchler, Martin Johns | 03/11/2015 | This chapter provided a broad overview of recent security testing techniques. |
| 2. | A security testing platform for Wireless Sensor Networks | Min Wei, Shuaidong Zhang, Keecheon Kim | 10/03/2016 | The test results show that the platform is a feasible platform for assessing device security levels in WSNs. |
| 3. | Vulnerability Analysis Using the Interactive Application Security Testing (IAST) Approach for Government X Website Applications | Hermawan Setiawan, Lytio Enggar Erlangga, Ido Baskoro | 29/01/2021 | Using the IAST approach, a total of 249 vulnerability risks were identified. |

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Literature Survey

| Sr. No. | Paper Title | Author Name | Date | Findings |
|---------|---|--|------------|--|
| 4. | Intelligent Testing in Software Industry | Anushka Lal, Girish Kuma | 03/11/2021 | This study aims to investigate the approach of intelligent testing for improving software testability. |
| 5. | Automated Cyber Security Testing Platform for Industrial Control System | Andrew Hahn, Daniel R. Sandoval, Raymond E. Fasano, Christopher Lamb | 23/10/2021 | A platform that incorporates these three components to provide the most accurate representation of actual NPP networks and controllers is developed in this paper. |

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Existing System

Hack The Box

Hack The Box is an online platform allowing security professionals to test their penetration testing skills and exchange ideas and methodologies with other members of similar interests. It contains several challenges that are constantly updated. Some of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge.

- **Advantages** - As an individual, they can complete a simple challenge to prove their skills and then create an account, allowing them to connect to HTB private network (HTB Net) where several machines await for them to hack them. By hacking machines they get points that help them advance in the rankings.
- **Disadvantage** – On this platform security professionals has to compete with others, so they invest their most of the time in competing with others rather than investing on their own skills.



<https://hackthebox.com/>

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

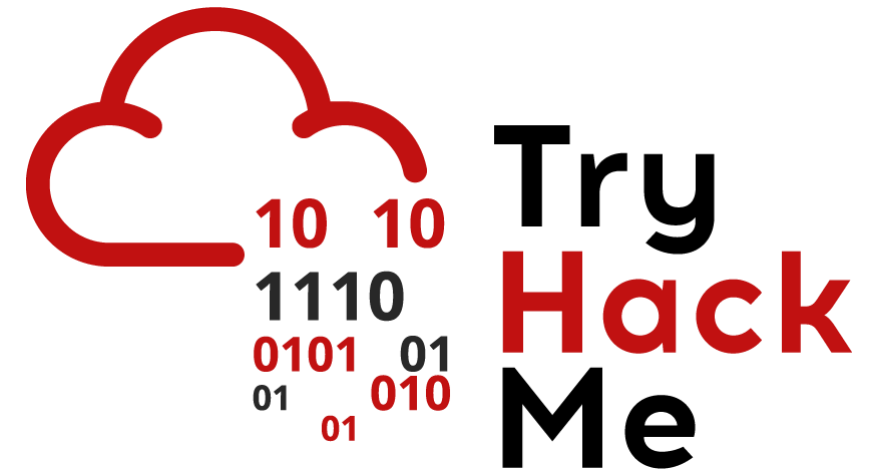


Existing System

TryHackMe

TryHackMe takes the pain out of learning and teaching Cybersecurity. Our platform makes it a comfortable experience to learn by designing prebuilt courses which include virtual machines (VM) hosted in the cloud ready to be deployed. This avoids the hassle of downloading and configuring VM's. Our platform is perfect for CTFs, Workshops, Assessments or Training.

- **Advantages** – Free basic learning and testing applications available to the masses.
- **Disadvantages** – For paid subscription is needed for intermediate or advanced learning and testing on the platform



<https://tryhackme.com/>

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Problem Statement

- **Cyber security** is a vast field and immerging daily. With increasing digital theft and cyber criminals, we need security tester and practitioner to help us tackle the increasing problem.
- It is necessary for them to learn testing without violating cyber laws.
- The vulnerable web application will provide a platform to learn and test their skills in their own local environment.



Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

Proposed System

- Vulnerable University is damn vulnerable application which any user can easily download from our GitHub page for free and run on their local system with single command.
- This application can also be used using Docker file for platform independency and without having need to download and install dependencies to run the application.
- Our application consists of different technologies and their associated vulnerabilities for not only testing but also for learning and understanding different bugs.

I. Objectives

1. To identify the threats in the web application, servers & websites.
2. To find potential vulnerabilities of the system and try to resolve those vulnerabilities.
3. To help in detecting to every possible security risk in the system.
4. Examine the impact occurs due to vulnerabilities.
5. To help the organizations and developer teams to resolving the security problem.
6. Improve the skills of the security professionals.
7. Introducing the various kind of hacking techniques without violating cyber laws.
8. Provide cyber education to students regarding technical and non-technical vulnerabilities.

Engineering

Management

Law

Schools

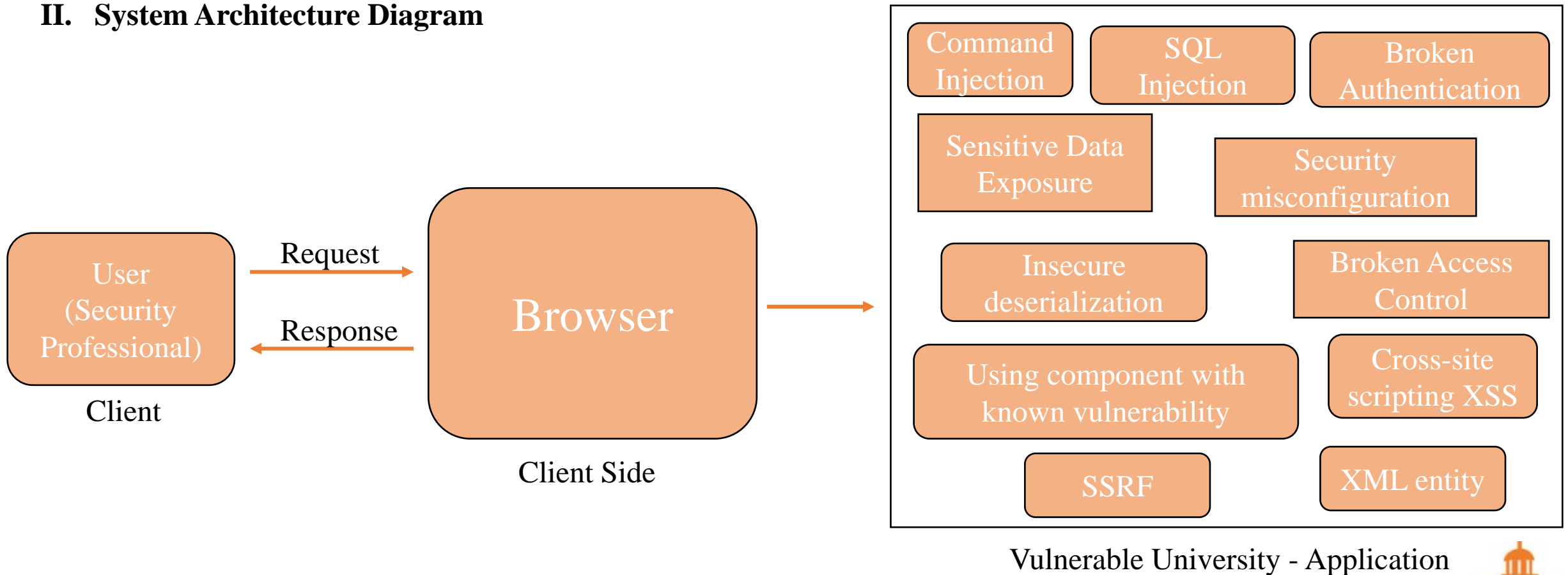
Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Proposed System

II. System Architecture Diagram



Engineering

Management

Law

Schools

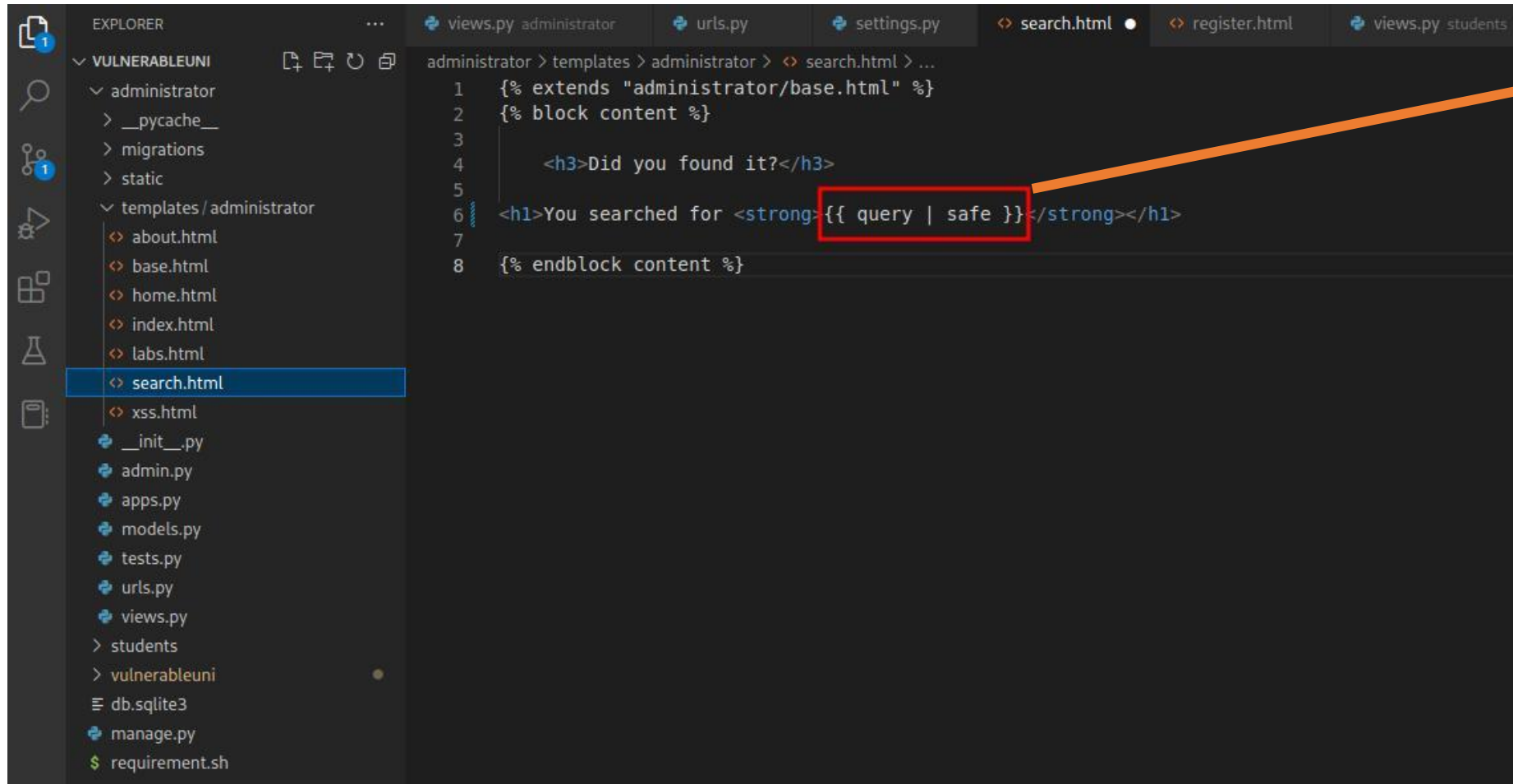
Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

RAISONI
GROUP OF INSTITUTIONS

Proposed System

III. Module



The screenshot shows a code editor with a file explorer on the left and a code editor on the right. The file explorer shows a project structure with a folder named 'VULNERABLEUNI' containing subfolders 'administrator' and 'students'. The 'administrator' folder contains a 'templates' subfolder, which in turn contains a 'search.html' file. The 'search.html' file is selected and its content is displayed in the code editor. The code is a Jinja2 template snippet. Line 6 contains the line: `<h1>You searched for {{ query | safe }}</h1>`. The expression `{{ query | safe }}` is highlighted with a red box. An orange arrow points from this box to the text 'Vulnerable Component' on the right.

```
1 {% extends "administrator/base.html" %}
2 {% block content %}
3
4     <h3>Did you found it?</h3>
5
6     <h1>You searched for <strong>{{ query | safe }}</strong></h1>
7
8 {% endblock content %}
```

Vulnerable
Component

Engineering

Management

Law

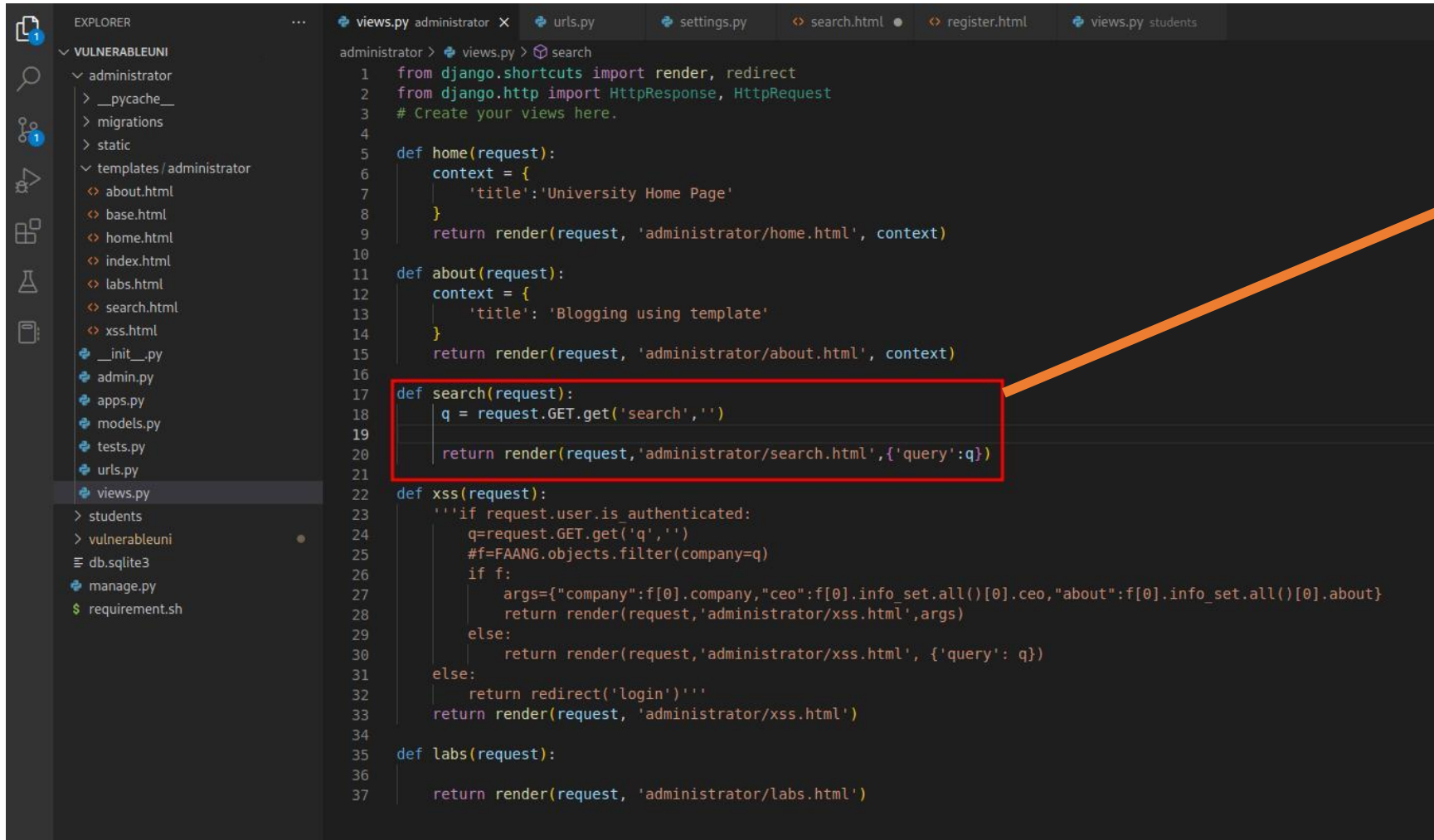
Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

Proposed System

III. Module



```
1 from django.shortcuts import render, redirect
2 from django.http import HttpResponse, HttpRequest
3 # Create your views here.
4
5 def home(request):
6     context = {
7         'title': 'University Home Page'
8     }
9     return render(request, 'administrator/home.html', context)
10
11 def about(request):
12     context = {
13         'title': 'Blogging using template'
14     }
15     return render(request, 'administrator/about.html', context)
16
17 def search(request):
18     q = request.GET.get('search', '')
19
20     return render(request, 'administrator/search.html', {'query': q})
21
22 def xss(request):
23     '''if request.user.is_authenticated:
24         q=request.GET.get('q','')
25         #f=FAANG.objects.filter(company=q)
26         if f:
27             args={"company":f[0].company,"ceo":f[0].info_set.all()[0].ceo,"about":f[0].info_set.all()[0].about}
28             return render(request,'administrator/xss.html',args)
29         else:
30             return render(request,'administrator/xss.html', {'query': q})
31     else:
32         return redirect('login')'''
33     return render(request, 'administrator/xss.html')
34
35 def labs(request):
36
37     return render(request, 'administrator/labs.html')
```

Vulnerable
Component

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA

Proposed System

IV. Technology Used

Django –

Django is free, open source and written in Python. We design application using Django because Django makes it easier to build application using Python. Django takes care of the difficult stuff so that we can concentrate on building our application. Django emphasizes reusability of components, also referred to as DRY (Don't Repeat Yourself), and comes with ready-to-use features like login system, database connection and CRUD operations (Create Read Update Delete).

Docker –

Docker is a set of platform as a service products that use OS-level virtualization to deliver software in packages called containers. The service has both free and premium tiers. The software that hosts the containers is called Docker Engine. By using this technology we make our application platform friendly. So, anyone can run this application on their own local system.

Engineering

Management

Law

Schools

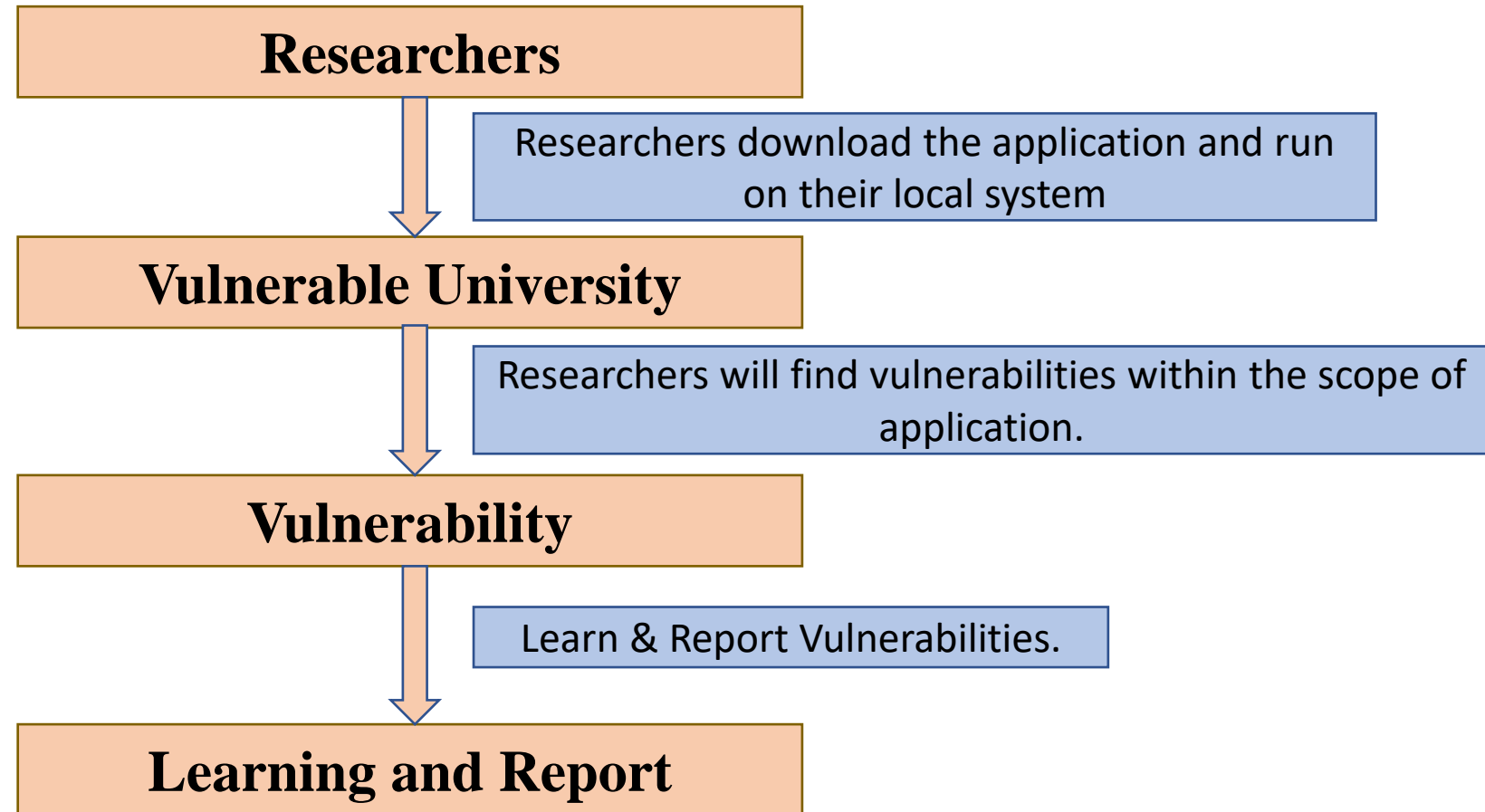
Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



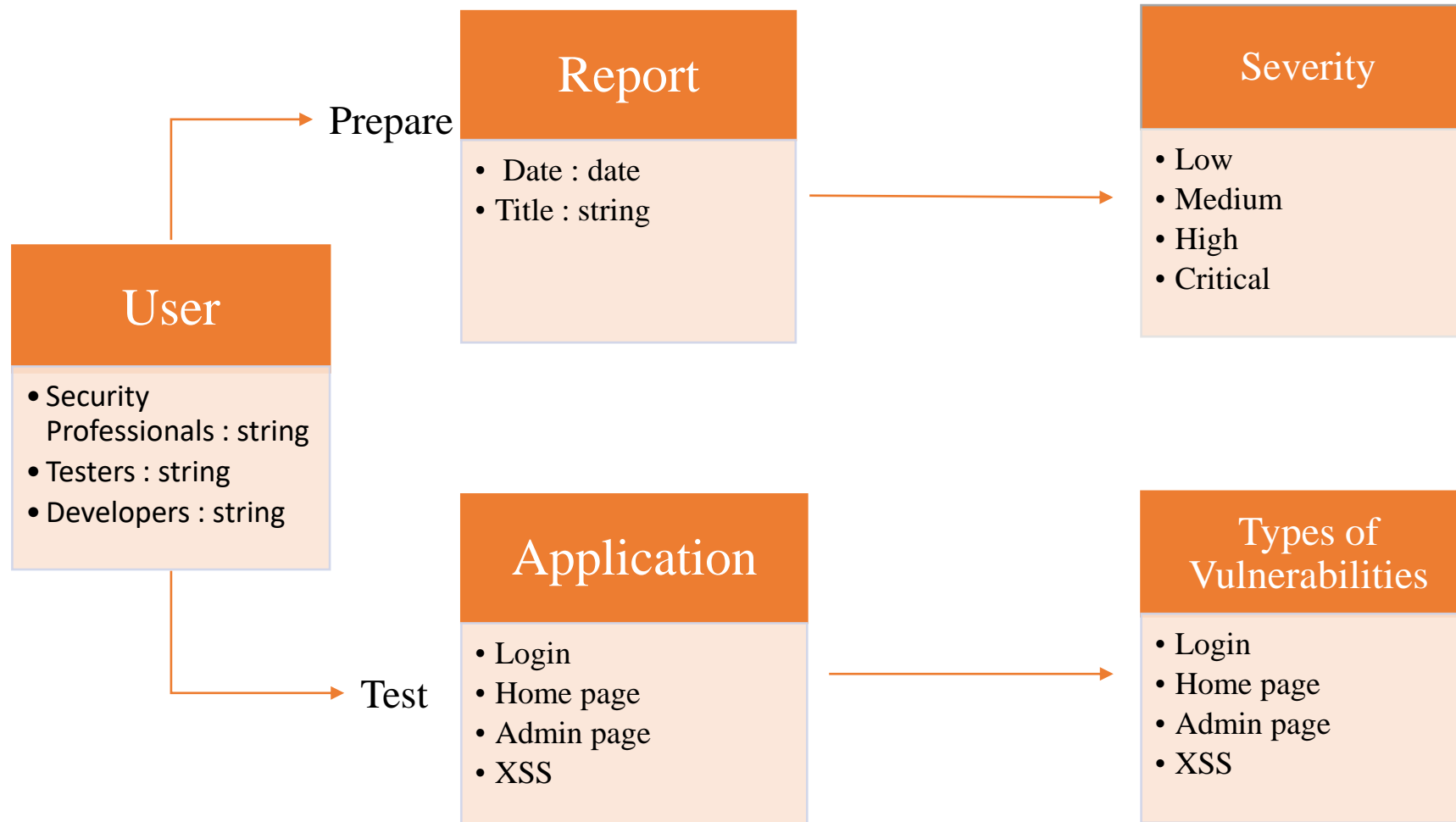
Proposed System

V. Block Diagram



Proposed System

VI. UML Diagram



Proposed System

VII. Hardware & Software Used

1. Hardware Requirement

- 1 TB HDD
- 4/8 GB RAM
- i5 or above processor

2. Software Requirement

- Operating System – Linux, Windows, Mac (platform independent)
- Web Browser – Chrome, Firefox, etc
- Docker
- GitHub
- Python - Django

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



RAISONI
GROUP OF INSTITUTIONS

Advantages & Disadvantages

Advantages –

- Vulnerable University is a platform, which have various kind of vulnerabilities their to practice.
- This application is free to for anyone and easily available for them.
- It is platform independent.
- This application is not only for testing or practicing but also for learning different types of bugs.

Disadvantages –

- Before accessing this application user must have some basic understanding of testing.
- Users can misuse this skills.

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Applications

- Security Professionals can brush up their skills, even can learn some different vulnerabilities.
- For developers, this application can help them to understand, how attackers can hack their application, they can understand the types of bugs.
- Students are able to practice finding technical and non-technical web-application vulnerabilities in their local environment

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Conclusion

- Cyber Security is method of protecting and securing the computer devices, network and program from cyber-attack. The importance of cyber security is rising.
- Cyber criminals are more sophisticated, changing the attacking approach and they are creating a really crucial conditions for organizations by affecting their image.
- Vulnerable university helps to enhance the skills of security professionals as well as this application helps to spread awareness about the ethical hacking amongst students. Anyone can easily get access of this free application and can run on their local environment. Students can learn required skills and can earn decent amount by finding valid bugs for many organizations on various platforms.

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



References

1. https://www.researchgate.net/publication/297918097_Security_Testing_A_Survey
2. <https://ieeexplore.ieee.org/document/7427093/metrics#metrics>
3. <https://www.cigniti.com/resource/white-papers/security-testing-tools-experiences-recommendations/>
4. <https://www.osti.gov/servlets/purl/1854691>
5. <https://securitytrails.com/blog/vulnerable-websites-for-penetration-testing>
6. <https://tryhackme.com/network/throwback>
7. <https://tryhackme.com>
8. <https://hackthebox.com>
9. <https://github.com/abhhi-101/vulnerable-university>

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



Thank You

Engineering

Management

Law

Schools

Other Courses

■ NAGPUR ■ PUNE ■ JALGAON ■ AMRAVATI ■ AHMEDNAGAR ■ CHHINDWARA



RAISONI
GROUP OF INSTITUTIONS